Chapter 1 (Part 2): Sets and Relations

Hamza MOUFEK

Algebra 1

October 2025

المدرسة الوطنية العليا في الأمن السيبراني
NATIONAL SCHOOL OF CYBERSECURITY

Outlines of this talk

- Sets
- Relations Between Sets
- Set Operations
- Cartesian Product ,Power Set and Partition of a Set
- Relations

Basic Concepts

Definition

A set is a collection of objects called elements or members of the set.

- If x is a member of the set A, we write :

$$x \in A,$$

and if x is a not member of the set A, we write

$$x \notin A.$$

- The empty set is the set that contains no elements. It is denoted by $\varnothing$ or $\{\}$
- Two sets are **equal** if they have exactly the same elements. In other words,

$$\mathbf{A} = \mathbf{B} \Longleftrightarrow (\mathbf{x} \in \mathbf{A} \Leftrightarrow \mathbf{x} \in \mathbf{B})$$

(that is, have exactly the same elements)

Examples

- the students in this classroom
- the points in a straight line
- $\{a, b, c\}$
- the set of Even numbers up to 50.

Basic Concepts

In set theory there are several description methods:

Listing :the set is described by listing all its elements
Example:$\{a, e, i, o, u\}$

Abstraction: the set is described through a property of its elements
Example:$A = \{x|\text{is a vowel of the Latin alphabet}\}$

Another way to discribe a set is to use predicate :

$$A = \{x|P(x)\}$$

This notation is also known as **set-builder** notation.

Examples

- $\{x \in \mathbb{R} \mid |x-2| < 1\}$,
- $\{z \in \mathbb{C} \mid z^5 = 1\}$,
- $\{x \in \mathbb{R} \mid 0 \leq x \leq 1\} = [0, 1]$
- $\{x \in \mathbb{R}|x^2 + 3x + 2 = 0\} = \{-1, -2\}$

Venn Diagrams: graphical representation that supports the formal description

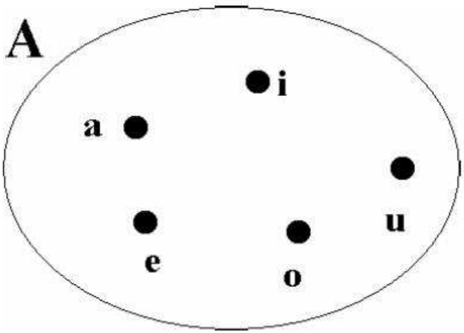

Figure: Venn diagram

Basic Concepts

Sets of Numbers

- $\mathbb{N} = \mathbb{Z}^+ =$ natural numbers $= \{0, 1, 2, 3, 4, ...\}$
- $\mathbb{Z} =$ integers $= \{....., -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$
- $\mathbb{Q} =$ rational numbers $= \{\frac{m}{n} | m, n \in \mathbb{Z} n \neq 0\}$
- $\mathbb{R} =$ real numbers
- $\mathbb{R} \diagdown \mathbb{Q} =$ irrational numbers
- $\mathbb{C} =$ complex numbers $= \{x + iy | x, y \in \mathbb{R}, \text{where } i = \sqrt{-1}\}$

Cardinality

Definition

The Cardinality $|\mathbf{A}|$ of a set $\mathbf{A}$ is the number of distinct elements of $\mathbf{A}$. If $|\mathbf{A}|$ is finite, then $\mathbf{A}$ is said to be finite. Otherwise, is said to be infinite.

Examples

- $|\varnothing| = 0$ while $|\{\varnothing\}| = 1$
- $|\{1, 2, 5\}| = 3$
- The set of prime numbers is infinite.

subsets

Definition

- We say that a set $\mathbf{A}$ is a subset of a set $\mathbf{B}$, and we write $\mathbf{A} \subset \mathbf{B}$, if every element of $\mathbf{A}$ is an element of $\mathbf{B}$.

$$\mathbf{A} \subseteq \mathbf{B} \Longleftrightarrow \forall \mathbf{x}, (\mathbf{x} \in \mathbf{A} \Longrightarrow \mathbf{x} \in \mathbf{B})$$

- Sets $\mathbf{A}$, $\mathbf{B}$ are equal, written $\mathbf{A} = \mathbf{B}$, if they have exactly the same elements. Equivalently:

$$\mathbf{A} = \mathbf{B} \Longleftrightarrow \mathbf{A} \subseteq \mathbf{B} \quad \text{and} \quad \mathbf{B} \subseteq \mathbf{A}$$

- $\mathbf{A}$ is a proper subset of $\mathbf{B}$ if it is a subset which is not equal. This can be written

$$\mathbf{A} \subsetneq \mathbf{B}$$

subsets

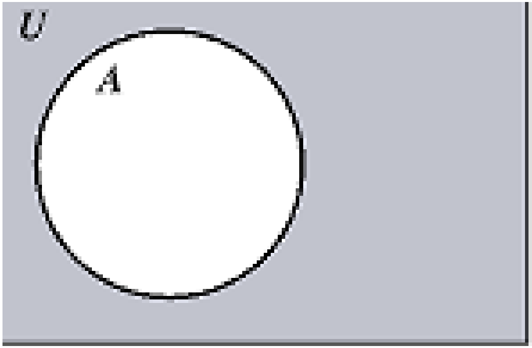

Figure: $\mathbf{A} \subsetneq \mathbf{B}$

subsets

Examples:

- $\{x \in \mathbb{R} | x^2 - 1 = 0\} \subset \{y \in \mathbb{R} | y^2 \in \mathbb{N}\}$
- $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
- $4\mathbb{Z} \subset 2\mathbb{Z}$

remark

We have then

$$\mathbf{A} \not\subseteq \mathbf{B} \Leftrightarrow \exists \mathbf{x} | \mathbf{x} \in \mathbf{A} \wedge \mathbf{x} \notin \mathbf{B}$$

Examples:
Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 5\}$. Then $A \not\subseteq B$ because $\exists 3 \in A$ and $3 \notin B$.

Here we collect several results relating to subsets.

Theorem

-1 If $|A| = 0$, then $A = \varnothing$.

-2 For any set A, we have $\varnothing \subset A$ and $A \subseteq A$

-3 If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$

Unions, Intersections, and Complements

Definition

- Let $A \subset U$ be a set. The complement of A is the set

$$A^C = \{x \in U : x \notin A\}.$$

This can also be written $U \setminus A$, $U - A$, or $\overline{A}$.

- If $B \subset U$ is some other set, then the complement of A relative B is

$$B \setminus A = \{x \in B, x \notin A\}$$

- The union of A and B is the set

$$A \cup B = \{x \in U : x \in A \vee x \in B\}.$$

- The intersection of A and B is the set

$$A \cap B = \{x \in U : x \in A \wedge x \in B\}.$$

- We say that A and B are disjoint if $A \cap B = \varnothing$.

Let A and B be sets:

- The **union** of A and B is the set $A \cup B = \{x : \ x \in A \ \cup \ x \in B\}$.

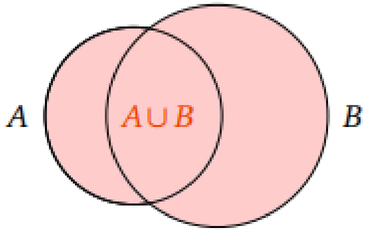

Figure: $\mathbf{A} \cup \mathbf{B}$

- The **intersection** of A and B is the set $A \cap B = \{x : \ x \in A \ \cap \ x \in B\}$.

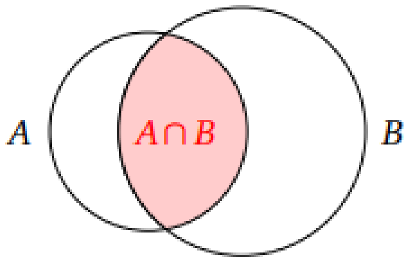

Figure: $\mathbf{A \cap B}$

- The **difference** of A and B is the set $A - B = \{x : \ x \in A \ \cap \ x \notin B\}$

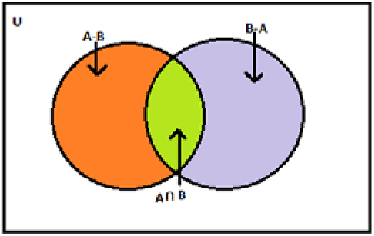

Figure: $\mathbf{A} - \mathbf{B}$

Unions, Intersections, and Complements

- The **symmetricdifference** of A and B is the set $A \triangle B = (A - B) \cup (B - A)$

  Note that $A - B$ is, in general, not equal to $B - A$
- The **complement** of A is the set $\overline{A} = \{x : \; x \notin A\} = E - A$

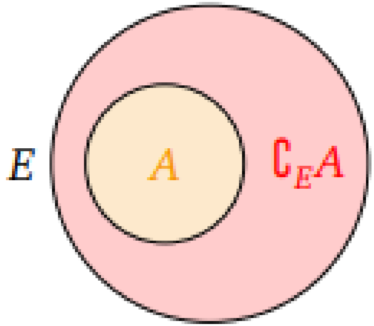

Figure: $\mathbf{A^C}$

Calculation Rules

Let A, B, C be set .Then :

-1 $\emptyset \cup A = A$ and $\emptyset \cap A = \emptyset$(**Identity**)

-2 $A \cap B \subseteq A \subseteq A \cup B$

-3 $A \cap B = B \cap A$ and $A \cup B = B \cup A$ (**Commutative properties**)

-4 $A \cap (B \cap C) = (A \cap B) \cap C$ (**Associative properties**)

-5 $A \cup (B \cup C) = (A \cup B) \cup C$ (**Associative properties**)

-6 $A \cup A = A \cap A = A$

-7 $A \subset B \Rightarrow A \cup C \subseteq B \cup C$ and $A \cap C \subseteq B \cap C$.

-8 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (**Distributive properties**)

-9 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (**Distributive properties**)

-10 $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ and $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$(**Morgan's Laws**) ,

-11 $\forall A, B \in \mathcal{P}(E), A \subseteq B \Rightarrow \overline{B} \subseteq \overline{A}$

Unions, Intersections, and Complements

Here are the drawings for the last assertion.

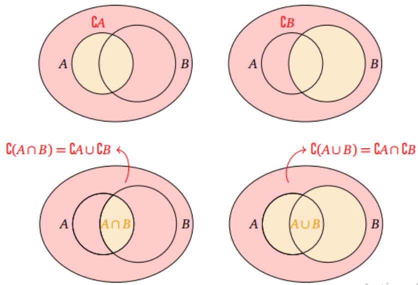

Figure: Morgan's laws

Cartesian Product

- Given two sets A and B, we define the Cartesian product of A and B as the set of ordered couples (a, b) where $a \in A$ and $b \in B$;formally,

$$A \times B = \{(a, b) : a \in A \text{ and} b \in B\}$$

- Notice that:$A \times B \neq B \times A$
- we have $(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$

Examples

- $A = \{1, 2\}|$ and $B = \{1, 2, 5\}$
  $A \times B = \{(1, 1), (1, 2), (1, 5), (2, 1), (2, 2), (2, 5)\}$
  $B \times A = \{(1, 1), (1, 2), (2, 1), (2, 2), (5, 1), (5, 2)\}$
- $\{1, 2, 7\}$ and $B = \{\emptyset, \{1, 5\}\}$
  $A \times B = \{(1, \emptyset), (1, \{1, 5\}), (2, \emptyset), (2, \{1, 5\}), (7, \emptyset), (7, \{1, 5\})\}$
- The Cartesian product $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is called the Cartesian plane.

- The Cartesian product can be computed on any number n of sets $A_1, A_2, \ldots.., A_n$, $A_1 \times A_2 \times \ldots \times A_n$ is the set of ordered $n-$tuple $(x_1, \ldots, x_n)$ where $x_i \in A_i$ for each $i = 1, \ldots, n$.
- These ordered systems are called triples for $n = 3$, quadruplets for $n = 4$ and $n-$tuples for n. We note it by $A_1 \times A_2 \times \ldots A_n$ or in abbreviation $\prod\limits_{i=1}^{i=n} A_i$. When $A_i = A$ the product $\prod\limits_{i=1}^{i=n} A_i$ is noted as A^n.
- like

$$A \times B \times C = \{(a, b, c), a \in A \wedge b \in B \wedge c \in C\},$$

$$A \times B \times C \times D = \{(a, b, c, d), a \in A \wedge b \in B \wedge c \in C \wedge d \in D\},$$

- $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R}$ (n times) is the Cartesian $n-$space

Power Set

There is a natural way to construct a family of sets. Take a set A. The collection of all subsets of A is called the power set of A and denoted by $\mathcal{P}(A)$.

Definition

For any set A,

$$\mathcal{P}(A) = \{B, B \subseteq A\}$$

Examples

$\mathcal{P}(\{1,2,5\}) = \{\emptyset, \{1\}, \{1,2\}, \{1,5\}, \{2,5\}, \{2\}, \{5\}, A\}$

Remark

$\mid \mathcal{P}(A) \mid = 2^{|A|}$

Partition of a Set

- Let X be a set.A partition of X is a collection of disjoint subsets of X such that their union is X.
- The collection of subset $A_1, A_2, ..., A_k$ forms a partition of X, if and only if:

$$A_i \neq \emptyset, \forall i \in \mathbb{N}$$

$$A_1 \cup A_2 \cup ... \cup A_k = X, \text{ and}$$

$$A_i \cap A_j = \emptyset \text{ for all } i \neq j.$$

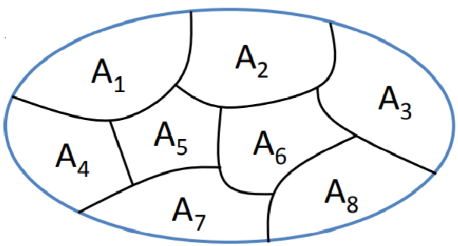

Figure: Partition of a set

Example

Let $E = \{1, 2, 3, 4\}$, if we take

$$A = \{1, \}, B = \{2, 3\}, C = \{4\}.$$

Ten

$$F = \{A, B, C\}$$

is a partition of E, but

$$F' = \{\emptyset, A, B, C\}$$

it is not a partition of E.

- In natural language relations are a kind of links existing between objects. Examples: ‘mother of’, ‘neighbor of’, “part of”, ‘is older than’, ‘is an ancestor of’, ‘is a subset of’, etc.
- A relation $\mathcal{R}$ on a set is defined by any subset Γ of $E \times E$. When$(x, y) \in \Gamma$, we say that is related to via $\mathcal{R}$, and we write $x\mathcal{R}y$.$\Gamma$is called «the graph of the relation $\mathcal{R}$»
- A binary relation on a set A is a subset $\mathcal{R} \subseteq A \times A$
- given$A = \{1, 2, 3, 4\}$,$B = \{2, 4, 6, 8, 10\}$ and $a\mathcal{R}b \Leftrightarrow a$ is a divisor of$b$, then $\Gamma = \{(1, 2), (1, 4), (1, 6), (1, 8), (1, 10), (2, 2), (2, 4), (2, 6), (2, 8), (2, 10), (3, 6), (4, 4), (4, 8)\}$

  is a graphe of the relation $\mathcal{R}$.

Examples

- Let$E = \mathbb{R}$ and define the relation $\mathcal{R}_1$ by

$$\forall x, y \in \mathbb{R}, x\mathcal{R}_1 y \Leftrightarrow x = y.$$

  The graph of $\mathcal{R}_1$ 1is :

$$\Gamma = \{(x, x), x \in \mathbb{R}\}$$

- Let$E = \mathbb{N}^*$,and define the relation $\mathcal{R}_2$ by

$$\forall (x, y) \in \mathbb{N}^*, x\mathcal{R}_2 y \Leftrightarrow x|y.$$

  We have

$$x|y \Leftrightarrow \exists k \in \mathbb{N}^* | y = kx$$

  The graphe of $\mathcal{R}_2$ is

$$\Gamma = \{(x, kx), x \in \mathbb{N}^*\}$$

- Let$E = \mathbb{N} \times \mathbb{N}, (a, b)\mathcal{R}_3(c, d) \Leftrightarrow a + d = b + c$

Properties

Definition

Let $\mathcal{R}$ be a relation on a the non emptyset E

- We say that $\mathcal{R}$ is reflexive if $x\mathcal{R}x$. for all $x \in E$.
- We say that $\mathcal{R}$ is symmetric if $x\mathcal{R}y \Rightarrow y\mathcal{R}x$. for all $(x, y) \in E^2$.
- We say that $\mathcal{R}$ is antisymmetric if $x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y$ for all $(x, y) \in E^2$.
- We say that $\mathcal{R}$ is transitive if $x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$ for all $(x, y, z) \in E^3$.

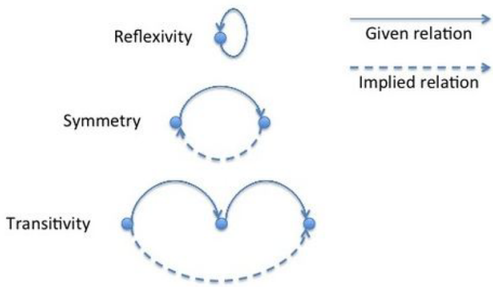

Figure: reflexive, symmetric, transitive

Properties

Example 1

Let $X = \mathbb{Z}$, and define a relation $\mathcal{R}$ by $x\mathcal{R}y \Leftrightarrow \gcd(x, y) = 1$. Let's consider what properties $\mathcal{R}$ satisfies.

- Reflexivity: NO.Take $\mid x \mid > 1$, then $\gcd(x, x) = x \neq 1$, so $x\mathcal{R}x$ is almost never true.
- Symmetry: YES. Since $\gcd(x, y) = \gcd(y, x)$, we definitely have symmetry.
- Antisymmetry: NO. Obviously we can't have symmetry and antisymmetry at the same time.
- Transitivity: NO. Take $x = 10, y = 9, z = 20$. Then we have $x\mathcal{R}y$ and $y\mathcal{R}z$, but we definitely don't get $x\mathcal{R}z$.

Properties

Example 2

Let $X = \mathbb{R}$, and define a relation $\mathcal{R}$ by $x\mathcal{R}y \Leftrightarrow x \leqslant y$. Let's consider what properties $\mathcal{R}$ satisfies.

- Reflexivity: yes. Certainly $x \leqslant x$ is always true.
- Symmetry: No. It doesn't make sense that $x \leqslant y \Rightarrow y \leqslant x$
- Antisymmetry: YES. If $x \leqslant y \wedge y \leqslant x$, it is standard to conclude that $x = y$.
- Transitivity: YES. If $x \leqslant y \wedge y \leqslant z$, we know that $x \leqslant z$.

Properties

Example 3

Let $X = \mathbb{N}^*$, and define a relation $\mathcal{R}$ by $x\mathcal{R}y \Leftrightarrow x|y$. Let's consider what properties $\mathcal{R}$ satisfies. Indeed,

- Reflexivity: yes. Certainly $x|x$ is always true.
- Symmetry: No. It doesn't make sense that $x|y \Rightarrow y|x$, let $x = 2$ and $y = 4$. We have 2 divides 4, but 4 doesnot divide 2, Therefore,$\mathcal{R}$ is not symmetric.
- Antisymmetry: YES. Indeed,

$$x|y \Leftrightarrow \exists k \in \mathbb{N}^* | y = kx$$

$$y|x \Leftrightarrow \exists k' \in \mathbb{N}^* | x = k'y$$

we have then

$$x = kk'x$$

It follows that

$$x(1 - kk') = 0$$

Since $x \neq 0$ then $1 - kk' = 0$. Now ,as k et k' are positive integers,we have

Example 3

$$kk' = 1 = k' = 1$$

Hence

$$x = y$$

- Transitivity: YES. If

$$x|y \Leftrightarrow \exists k_1 \in \mathbb{N}^* | y = k_1 x$$

and

$$y|z \Leftrightarrow \exists k_2 \in \mathbb{N}^* | z = k_1 y,$$

we have then

$$z = k_1 k_2 x$$

Setting $k_3 = k_1 k_2$, we have $z = k_3 x$ with $k_3 \in \mathbb{N}^*$ Therefore $x\mathcal{R}z$.

Definition

Definition

A relation $\mathcal{R}$ on X is called an equivalence relation if it is reflexive, symmetric, and transitive.

Example

- The equality relation $\mathcal{R}$is an equivalence relation.
- The divisibility relation is not an equivalence relation.(example 3)
- The relation of example 1 is note an equivalence relation.

Equivalence class

Let $\mathcal{R}$ be an equivalence relation on a set X, a is an item in X.Equivalence class is :

- The set of all elements that are related to an element a of X
- $\overline{a}$ denotes the equivalence class of a with respect to $\mathcal{R}$.
- $\overline{a} = \{s | (a, s) \in \Gamma\}$ with Γ is graphe of $\mathcal{R}$.
- Consider $X = \{1, 2, 3, 4\}$ and its equivalence relation

$$\Gamma = \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(2,3),(3,2),(1,3),(3,1)\}$$

$$\overline{1} = \{1, 2, 3\}$$

$$\overline{2} = \{2, 1, 3\}$$

$$\overline{3} = \{3, 2, 1\}$$

$$\overline{4} = \{4\}$$

- We have

$$\overline{a} = \overline{b} \Leftrightarrow a\mathcal{R}b$$

quotient set

Definition

Let $\mathcal{R}$ be an equivalence relation on a non emptyset E.The set of equivalence classes is called the quotient set of E modulo$\mathcal{R}$.It is denoted by $E/\mathcal{R}$.

Example

We define on the set of integers $\mathbb{Z}$ the relation $\mathcal{R}$, called congruence relation modulo 3, by

$$\forall x, y \in \mathbb{Z}, x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z}, x - y = 3k.$$

This is an equivalence relation. There are three equivalence classes :

$$\bar{0} = \{3k; k \in \mathbb{Z}\}$$

$$\bar{1} = \{3k + 1; k \in \mathbb{Z}\}$$

$$\bar{2} = \{3k + 2; k \in \mathbb{Z}\}$$

So we have

$$E/\mathcal{R} = \mathbb{Z}/\mathcal{R} = \{\bar{0}, \bar{1}, \bar{2}\}$$

Remark In these example ,when x is related to ,we writ:

$$x \equiv y\,[3]$$

and we read this as **"x is congruent to y modulo 3"**.

Fundamental Properties

Let $\mathcal{R}$ be an equivalence relation on the non empty set E.Then we have :

- If $y \in \overline{x}$, then $\overline{x} = \overline{y}$
- For all $x, y \in E, x\mathcal{R}y \Leftrightarrow \overline{x} = \overline{y}$.
- If $u, v \in \overline{x}$,then $u\mathcal{R}v$.
- For all $x, y \in E$, we have $\overline{x} = \overline{y}$ or $\overline{x} \cap \overline{y} = \emptyset$.
- Let E be a non empty set and let $\mathcal{R}$ be an equivalence relation on E .Then the quotient set $E/\mathcal{R}$ forms a partition of E.
- Conversely, every partition of E defines an equivalence relation on E.

Definition

Let E be a non empty set, and let $\mathcal{R}$ be a relation defined on E.$\mathcal{R}$ is said to be an order relation if it is reflexive, antisymmetric and transitive.

Example

- The equality relation .$\mathcal{R}$ is an order
- let A a set and $\mathcal{P}(A)$.$\mathcal{R}$ is defined on $\mathcal{P}(A)$ by

$$B\mathcal{R}C \Leftrightarrow B \subseteq C$$

  $\mathcal{R}$ is an ordre relation.
- Let $\mathcal{R}$ is defined on $\mathbb{N}$ by

$$a\mathcal{R}b \Leftrightarrow a|b$$

  is an ordre relation.

Partial And Total Order

Definition

Let E be a non empty set.An order relation defined on E, denoted by $\mathcal{R}$,is said to be a total order relation if we have

$$\forall x, y, \in E, x\mathcal{R}y \vee y\mathcal{R}x$$

We then say that $(E, \mathcal{R})$ is a totally ordered set.

Definition

When the order is not total, we say it is partial.

Example

The usual order $\leq$ on the set of real numbers is a total order relation, since we have

$$\forall x, y \in \mathbb{R}, x \leq y \vee y \leq x$$

The inclusion relation $\mathcal{R}$ defined on $\mathcal{P}(E)$ by

$$B\mathcal{R}C \Leftrightarrow B \subseteq C$$

is a partial order relation. Indeed, taking

$$E = \{1,2,3,4\}, \quad A = \{3\}, \quad B = \{1,2\}$$

we have

$$(A \nsubseteq B \wedge B \nsubseteq A).$$